AMENDMENTS TO THE SPECIFICATION

Please replace the paragraph beginning on page 2, line 14 and ending on page 2, line 16 with the following amended paragraph:

-- Access to premises in emergency or potential emergency situations, such as by fire departments in the event of a fire alarm, usually requires forced entry [[,]] if normally-authorized persons are not available to unlock doors, thereby causing structural damage and consequent repair expenses.--

Please replace the paragraph beginning on page 3, line 11 and ending on page 3, line 24 with the following amended paragraph:

-- According to one aspect of the present invention, there is provided a system for door access control and key management ~~system in which a number of doors and door users are involved~~. The system ~~comprises~~ includes: ~~(a) a communications network; (b)~~ (1) a ~~door/key~~ door administering system for ~~storing a key unique to each of the users,~~ administering access to one or more doors, the door administering system having: (a) a module for managing access privilege of one or more individuals for each door and assigning access authorization to each individual for the door, (b) a door database for storing [[an]] a door identification ~~code unique~~ uniquely assigned to each ~~of the doors~~ door and information on each authorized individual for each door, ~~and for assigning access authorization to at least one user for each door, the door/key administering system being communicatively connected to the communications network;~~ and (c) a module for changing data stored in the door database; (2) a key administering system for administering one or more keys separately from the administration of the access to the door, each key being uniquely assigned to a key owner, the key administering system having:(d) a key database for storing one or more keys for each key owner, and (e) a module for changing data stored in the key database, ~~(c)~~ (3) a door ~~lock/control~~ control/lock assembly mounted on each door, the door control/lock assembly, the door administering system and the key administering system communicating with each other through a communications network, the door control/lock assembly for ~~reading the key~~ identifying a user key when it is presented by ~~the~~ a user~~, for verifying that the key has access authorization~~, and for operating the door ~~in response to~~ based on ~~the authorization for~~ ~~access~~ access privilege of the

user when the identified key of the user is the key of a key owner who is an authorized individual having access authorization to the door~~, the door lock/control assembly being communicatively connected to the door/key administering system via the communications network; (d) whereby a user can gain access to the doors authorized to the user with a unique key and each door can provide access to the user or users assigned thereto~~.--

Please replace the paragraph beginning on page 3, line 25 and ending on page 4, line 5 with the following amended paragraph:

-- According to ~~another~~ a further aspect of the present invention, there is provided a method of ~~controlling access to a plurality of doors by a plurality of door users~~ implementing door access control and key management via a communications network. The method ~~comprises~~ includes: steps of: (1) at a door server, administering access to one or more doors, including: (a) managing access privilege of one or more individuals for each door and assigning access authorization to each individual for the door; and ~~(a)~~ (b) at a door database, storing a ~~unique~~ door identification ~~code~~ uniquely assigned [[for]] to each ~~of the~~ door[[s]] ~~in a server;~~ and information on each authorized individual for each door, data stored in the door database being updatable; (2) at a key server, administering one or more keys separately from the administration of the access to the door, each key being uniquely assigned to a key owner, including:~~(b)~~ (c) at a key database, storing ~~a unique key signature~~ one or more keys for each ~~of the users in the server~~ key owner, the keys being implemented by key signatures, data stored in the key database being updatable; ~~(c) assigning to each door the unique keys having access authorization to the respective doors;~~ (3) at a door control/lock assembly, identifying a user key presented by a user; [[(d)]] (4) comparing ~~a user's key detected at the door to the keys having access authorization to the door in the server~~ the identified key to the keys of the key owners and verifying that the identified key is a key of a key owner who is an authorized in individual having access authorization to the door; ~~(e) authorizing access to the door; and~~ (5) operating the door based on the access privilege of the individual, ~~(f)~~ wherein the authorization step is carried out through the communications network between the

door server and the key server ~~and each user can gain access to the doors authorized to the user with a unique key and each door can provide access to the user or users assigned thereto.~~

Please replace the paragraph beginning on page 4, line 6 and ending on page 4, line 18 with the following amended paragraph:

-- According to ~~another~~ a further aspect of the present invention, there is provided a system architecture for controlling ~~a plurality of~~ door access ~~control~~ and key management ~~systems~~. The system architecture ~~comprises~~ includes: (a) [[the]] a plurality of door access control and key management systems noted above, the systems being communicatively and operatively connected to a communication network; and (b) a Meta server being adapted to serve as an address reference among the door ~~access control~~ administering system and the key management system[[s]], which are separately part of each door access control and key management system, the Meta server being communicatively and operatively connected to each of the door access control and key management systems via the communications network, wherein the Meta server contains the address of each separate door ~~access control~~ administering system and key ~~management~~ administering system ~~and~~ each with its associated unique key ID codes and unique door ID codes, and each door access control and key management system contains the address of the Meta server such that any key owner, whose keys are administered by any key administrating system, can be granted access privileges at any door which is administered by any door administering system.--

Please replace the paragraph beginning on page 4, line 26 and ending on page 4, line 27 with the following amended paragraph:

-- FIGURE 1 illustrates a door access control and key management system with a door administering system and a key administering system according to one embodiment of the present invention;--

Please replace the paragraph beginning at page 5, line 14 and ending on page 5, line 23 with the following amended paragraph:

-- Referring to Fig. 1, the system generally comprises a door control/lock assembly 20, a key administering system 40, a door administering system 60, and a communications network 80. The door control/lock assembly 20 is mounted on each door and communicatively connected to the key and door administering systems 40 and 60 via the communications network 80. In practice, the door administering system 60 and the key administering system 40 can be implemented as one single system equipped with the appropriate software program for carrying out both functions for the convenience of people who are door administrators, who control doors and the access thereto, and who also have keys authorized for access for the doors that they administer or for doors to which access is controlled by other door administrators. In general, the door control/lock assembly 20 identifies a user 32 wanting to gain access to a door 30, and communicate with the key and door administering systems 40 and 60 to obtain authorization for access thereto. --

Please replace the paragraph beginning at page 6, line 3 and ending on page 6, line 11 with the following amended paragraph:

-- The connection between the communications network 80 and the door ~~lock/control~~ control/lock assembly 20 can be accomplished via a wireless communication line. In such a case, an intermediate wireless transmitter/receiver 82 between them is provided as illustrated in Fig. 1. The means of wireless communication includes Bluetooth® or other short-range wireless communications circuitry, or a network access module consisting of Bluetooth® wireless communications circuitry, an Ethernet network interface and a battery backed up power supply. The network access module is located at an Ethernet port within the range of the Bluetooth® or other short-range wireless communications circuitry. --

Please replace the paragraph beginning at page 6, line 17 and ending on page 6, line 30 with the following amended paragraph:

-- Fig. 2 presents a detailed view of the door control/lock assembly 20 of the system 10. As illustrated in Figs. 1 and 2, the door control/lock assembly 20 mounted on each door 30 includes an electric door lock 22, an identification device 24, an embedded controller 28, a communicating means 26, and a battery for supplying power. The communicating means 26 establishes two-way communications with the communication network 80 via a wireless transmitter/receiver 82. The embedded controller 28 has appropriate software for

controlling the door control/lock assembly 20 and any communications with other system components via the communications network 80. During operation, the door control/lock assembly 20 transmits via the communication network the identification data read by the identification device 24 to the key-door administering systems 40 and 60 and receives messages or signals from the administering systems as to whether the identified key is authorized. Details of the operation will be hereafter described. --

Please replace the paragraph beginning at page 7, line 25 and ending on page 8, line 5 with the following amended paragraph:

-- In the door ~~lock/control~~ control/lock assembly 20, the embedded controller 28 runs appropriate software for controlling the assembly 20 and carrying out an identification/authorization process by cooperating with the identification device 24 and communicating with the door and key server systems 40 and 60 via the communications network 80. Various identification/authorization software applications are well known in the art and any suitable one can be used. The embedded controller 28 comprises a local database or a memory 28a as shown in Fig. 2. The local database or memory 28a stores, for example, data of the most recent and most frequent users of the door in encrypted form for security reasons. These data serve to speed up authorization process, or provides back-up capability in the event that the connection between the door assembly 20 and the administering systems 40 and 60 failed or is disrupted for any reason. --

Please replace the paragraph beginning at page 8, line 18 and ending on page 8, line 30 with the following amended paragraph:

-- The door ~~lock/control~~ control/lock assembly 20 and the door server system 60 work together to provide a number of functions. For example, the door server system 60 records all uses of the door lock 22, including authorized entries and unauthorized attempts to enter. The door server system 60 also provides the necessary controls and communications capability to allow the door administrator to configure various security settings of the operation of the door control/lock assembly 20, in addition to the basic authorization settings of which keys are allowed to unlock which doors. These security settings include such functions as to who is authorized at specific times. Other additional functions include settings as to who is to be notified in the event of an alarm of low battery condition or a detection of hardware

failure condition and how such notification is to take place (e.g., e-mail, pager, automated phone call, or the like.) Such factors as the amount of lead-time to report that low battery condition can also be set. --

Please insert the following new paragraph after the paragraph beginning at page 10, line 1 and ending on page 10, line 6:

-- As is the situation for the door server systems and door administrators, a single key server system can provide these functions for a number of keys controlled by the same key administrator, or multiple key servers can be used. The same key server can also provide these functions for a number of different key administrators, but each key administrator is prevented from accessing the information pertaining to keys controlled by others. Any number of key server systems can run on the system at the same time. --

Please replace the paragraph beginning at page 10, line 18 and ending on page 11, line 2 with the following amended paragraph:

-- The system of Fig. 1 provides security means to control access by persons to building, rooms or vehicles, while gathering useful information. The system provides a means <u>for one or more door administrators</u> to allow a person access to some locations, while, at the same time, excluding access to other locations, this may be accomplished with only one access key per individual <u>as defined in that person's key server system database 42</u>. Such access privileges can be variable according to time. The system provides a means to change the security settings such as access privileges of an individual quickly and easily from any location where an Internet connection and browser software are available. Information gathered by the system includes the time of all attempts to access the door and the identification of the individual attempting such access (if known) or the fact that an unknown individual attempted to gain access. Furthermore, the access privileges associated with the 'key' may be easily changed as circumstances change. This allows people potential to have only one 'key' to open all of the doors in their lives while, at the same time, increasing security and convenience<u>, since each person can be their own key administrator</u>. --

Please replace the paragraph beginning at page 11, line 3 and ending on page 11, line 19 with the following amended paragraph:

-- To deal with the occasional instance that the communications network 80 is not available and to speed up access for frequent users of a door, a local database 28a of frequent and most recent user authorized key signatures is stored in encrypted form in the door ~~lock/control~~ control/lock assembly 20 itself. Before sending a request message for authorization over the communications network 80 to the door server system 60, the embedded controller 28 in the door ~~lock/control~~ control/lock assembly 20 checks its own local database 28a and unlocks the door if a match is found between the signature of the key being presented and one that is stored in the local database 28a. The information that this action has taken place is then transmitted to the door server system 60 for storage subsequent to the door having been unlocked. Periodically the authorized keys in the local database 28a of the door assembly 20 are confirmed between the door assembly 20 and the door server system 60 by a series of encrypted messages over the communications network 80. This confirmation process can be initiated by the door ~~lock/control~~ control/lock assembly 20, or the door administering system or server 60. If a key signature that has been authorized is no longer authorized, then the key signature is removed from the local database 28a of the embedded controller of the door assembly 20. --

Please replace the paragraph beginning at page 12, line 1 and ending on page 12, line 7 with the following amended paragraph:

-- As well, alarm devices such as motion detectors, smoke detectors, or water detectors etc. can be installed in the door ~~lock/control~~ control/lock assembly 20. The alarm device communicates with the door server system 60, which in turn communicates the alarm administrator according to instructions included in the database 62. Any other additional alarm components can be provided and configured to signal their condition in various ways and to monitor multiple locations that can be altered easily over time. --

Please replace the paragraph beginning at page 12, line 24 and ending on page 12, line 31 with the following amended paragraph:

-- The door control/lock assembly 20 can also include a digital camera (still or video) that is configured to provide an image of the individual attempting to gain access to a person assigned to make human ~~judgements~~ judgment on whether such individuals, not identified by the system should be allowed access. The judging

person may then allow the individual in, if desired, by signalling the door control/lock assembly 20 from the Web browser 52. The camera may also be configured to record in the network databases, an image of all individuals attempting to gain access. --

Please replace the paragraph beginning at page 13, line 12 and ending on page 13, line 17 with the following amended paragraph:

-- Each door access control and key management system 110a or 110b involves a plurality of doors and door users, and includes a door ~~lock/control~~ control/lock assembly mounted on each door, a door/key administering system comprised of a door administering system and a separate key administering system, and a communications network communicatively interconnecting the door ~~lock/control~~ control/lock assemblies and the administering system, as noted above in conjunction with the first embodiment of the invention of Fig. 1. --

Please replace the paragraph beginning at page 13, line 28 and ending on page 13, line 30 with the following amended paragraph:

-- Also, each door access control and key management system, i.e., each door/key administering system knows the location (i.e. network address) of the Meta server 140. The administering system contains the address of the Meta server 140. --

Please replace the paragraph beginning at page 14, line 11 and ending on page 14, line 14 with the following amended paragraph:

-- Therefore, the door access control and key management system 110a communicates with other system 110b via the Meta server 140 such that the system 110a can provide access to its own doors for a user or users from other system 110b and whose unique key ID numbers are stored on the other system. --

Please replace the paragraph beginning at page 16, line 4 and ending on page 16, line 8 with the following amended paragraph:

-- If a 'key' is lost or stolen it can be quickly and easily replaced for all its uses with no chance that the lost or stolen 'key' may be used by unauthorized persons. The replacement is effected by the key administrator accessing the key database via a browser and deleting or deactivating the unique key ID number associated with

the lost or stolen key, and adding a new unique key ID number associated with a replacement key. This new key is then propagated to the access control databases. Attempts by someone to use the lost or stolen 'key' can be reported to the key server database owned by the rightful key owner and such information may be useful in locating the missing key and possibly in apprehending the thief. --

Please replace the paragraph beginning at page 16, line 19 and ending on page 17, line 2 with the following amended paragraph:

-- The system allows the possibility for individuals to have one key that can be used for multiple situations, including their residences, various work situations, vehicles or any other places to which they may need access on a regular or occasional basis. These access privileges can be altered or scheduled easily and quickly to apply to specific times or to adapt to changing circumstances. Such changing circumstances may include moving to a new house, acquiring vacation property, changing jobs, acquiring a new vehicle, renting a vehicle, renting a hotel room, temporarily accessing the house of a friend or neighbour, or losing a 'key'. In the case of a lost or stolen 'key' (where biometric identification systems are not being used) the old key can be cancelled for all of its uses and a new 'key' can be authorized quickly and easily from any place where an Internet connection and browser software are available. Each individual can act as the door administrator for doors under their control, such as those in their house or car, and can act as their own key administrator, such that door administrators for, say, their place of work, their friends or relatives, can grant them access to doors for which these other door administrators administer access privileges. --